

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-312317

(43)Date of publication of application : 25.10.2002

(51)Int.Cl.

G06F 15/00

H04L 9/08

H04L 9/32

(21)Application number : 2001-112740

(71)Applicant : CASIO COMPUT CO LTD

(22)Date of filing : 11.04.2001

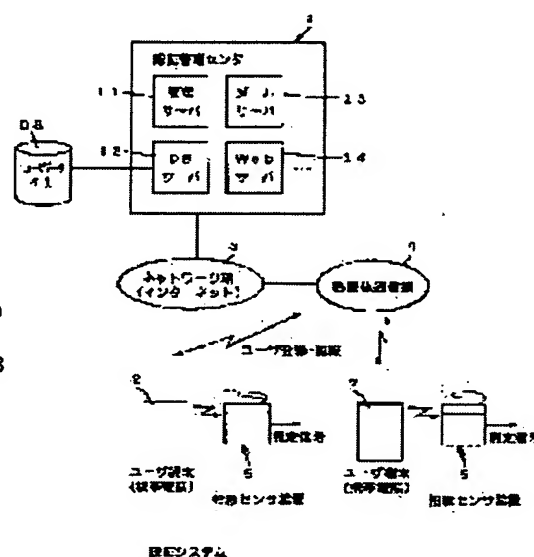
(72)Inventor : AKAO HIDETOSHI

## (54) CERTIFICATION SYSTEM AND CERTIFICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To realize a certain security management capable of effectively protecting a user certification information by dividing the user certification information for a setting registration to a plurality of constitution elements and dispersely managing them.

SOLUTION: A certification management center 1 divides the user certification information sent from a fingerprint sensor device 5 through a user terminal 2 at the time of registration of the user and allots one constitution element of respective constitution elements of the user certification information divided to a registration information at a system side and the other constitution element to a registration information set in the user terminal 2. The registration information in the user terminal 2 is obtained and the registration information at the system side is obtained from a user data base DB at the time of certification of the user. After the original user certification information is produced and restored based on the registration information in the user terminal 2 and the registration information at the system side obtained, the user certification is carried out by comparing the user certification information restored with the user certification information inputted at the time of certification of the user.



## LEGAL STATUS

[Date of request for examination] 23.08.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号  
特開2002-312317  
(P2002-312317A)

(43)公開日 平成14年10月25日(2002. 10. 25)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 8 5 3 3 0 F 5 J 1 0 4
H 0 4 L 9/08 9/32		H 0 4 L 9/00	6 7 3 Z 6 7 3 D 6 7 5 D

審査請求 未請求 請求項の数 8 O L (全 11 頁) 最終頁に続く

(21)出願番号 特願2001-112740(P2001-112740)

(22)出願日 平成13年4月11日(2001. 4. 11)

(71)出願人 000001443

カシオ計算機株式会社

東京都渋谷区本町1丁目6番2号

(72)発明者 赤尾 英俊

東京都羽村市栄町3丁目2番1号 カシオ  
計算機株式会社羽村技術センター内

(74)代理人 100073221

弁理士 花輪 義男

Fターム(参考) 5B085 AA08 AE26 BA07

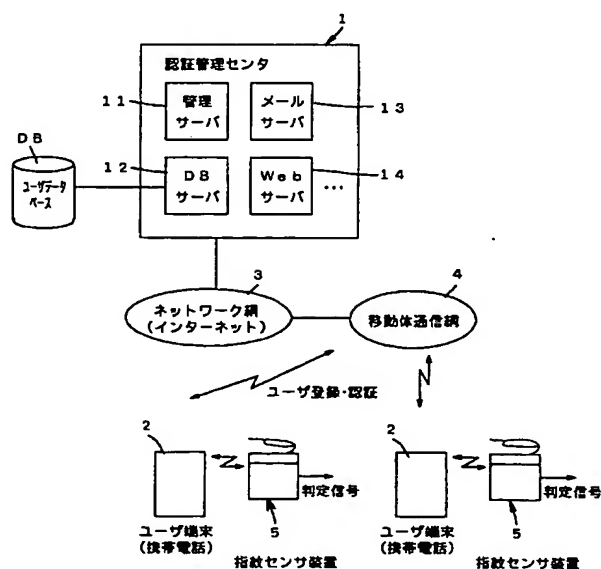
5J104 AA08 EA03 EA13 KA01 MA01  
NA05

(54)【発明の名称】 認証システムおよび認証方法

(57)【要約】

【課題】設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理することで、そのユーザ認証情報を効果的に保護することができる確実なセキュリティ管理を実現できるようにする。

【解決手段】認証管理センタ1は、ユーザ登録時に、指紋センサ装置5からユーザ端末2を介して通信されて来たユーザ認証情報を分割し、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報、他方の構成要素をユーザ端末2内に設定する登録情報として割当てる。ユーザ認証時に、ユーザ端末2内の登録情報を取得すると共に、ユーザデータベースD Bからシステム側の登録情報とを取得し、取得したユーザ端末2内の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元した後、復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行う。



認証システム

**【特許請求の範囲】**

【請求項 1】 ユーザ認証時に入力されたユーザ認証情報と、予め設定登録されているユーザ認証情報とを照合することによってユーザ認証を行う管理センタ装置と、ユーザ所有のユーザ端末とが通信ネットワークを介して接続されてなる認証システムであって、ユーザ認証情報を分割する分割手段と、この分割手段によって分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素を前記ユーザ端末内に設定する登録情報として割り当てて分割情報割当手段と、ユーザ認証を行う場合に、そのユーザ端末内に設定されている登録情報を取得すると共に、前記システム側に設定されている登録情報とを取得する登録情報取得手段と、この登録情報取得手段によって取得したユーザ端末内の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元する復元手段と、この復元手段によって復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行うユーザ認証手段と、を具備したことを特徴とする認証システム。

【請求項 2】 複数のユーザに対応してそれらのユーザ認証情報をそれぞれ設定登録する場合において、前記分割手段によって分割されたユーザ認証情報の構成要素をユーザ側の登録情報として当該ユーザ端末内に設定させる際は、その登録情報がシステム側のどの登録情報に対応するかを示す為の識別情報を含めて当該ユーザ端末内に設定させ、ユーザ認証を行う場合に前記登録情報取得手段は、そのユーザ所有のユーザ端末内に設定されている登録情報と共に前記識別情報を取得し、この識別情報に基づいて対応するシステム側の登録情報を取得する、ようにしたことを特徴とする請求項 1 記載の認証システム。

【請求項 3】 ユーザ認証を行った後において、前記分割手段は、前回の分割方法とは異なる方法でユーザ認証情報を再分割し、前記分割情報割当手段は、この分割手段によって再分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素をユーザ端末内に設定するユーザ側の登録情報として割り当てることにより、前回のユーザ側の登録情報とシステム側の登録情報の内容を変更する、ようにしたことを特徴とする請求項 1 記載の認証システム。

【請求項 4】 ユーザ認証が行われる毎に、前記分割手段は、ユーザ認証情報の分割位置をランダムに決定すると共に、この決定された分割位置にしたがってユーザ認証情報を再分割する、ようにしたことを特徴とする請求項 3 記載の認証システム。

【請求項 5】 ユーザの特徴情報をユーザ認証情報として検知する検知装置を設け、この検知装置とそのユーザ所持の携帯通信装置との間で近距離無線通信を行うと共

に、この携帯通信装置は、前記検知装置によって検知されたユーザ認証情報を受信して前記管理センタ装置へ送信し、前記管理センタ装置は、前記携帯通信装置から送信されて来たユーザ認証情報を分割すると共に、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素を前記ユーザ端末内に設定する登録情報として割り当て、ようにしたことを特徴とする請求項 1 記載の認証システム。

【請求項 6】 前記分割手段は、ユーザ認証情報を複数の分割位置で分割し、前記分割情報割当手段は、前記複数の分割位置によって細かく分割されたユーザ認証情報の各構成要素のうち、システム側に割り当てべき構成要素と、ユーザ端末内に割り当てべき構成要素とを選択決定する、ようにしたことを特徴とする請求項 1 記載の認証システム。

【請求項 7】 コンピュータに対して、ユーザ認証情報を分割する機能と、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素を前記ユーザ端末内に設定する登録情報として割り当てると共に、ユーザ認証を行う場合に、そのユーザ端末内に設定されている登録情報を取得すると共に、前記システム側に設定されている登録情報とを取得する機能と、取得したユーザ端末内の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元する機能と、復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行う機能と、を実現させるためのプログラム。

【請求項 8】 ユーザ認証を行う管理センタ装置と、ユーザ所有のユーザ端末とが通信ネットワークを介して接続されているシステム環境において、ユーザ認証時に入力されたユーザ認証情報と、予め設定登録されているユーザ認証情報とを照合することによってユーザ認証を行う認証方法であって、ユーザ認証情報を分割すると共に、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素を前記ユーザ端末内に設定する登録情報として割り当て、ユーザ認証を行う場合に、そのユーザ端末内に設定されている登録情報を取得すると共に、前記システム側に設定されている登録情報とを取得し、取得したユーザ端末内の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元し、復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行う、ようにしたことを特徴とする認証方法。

**【発明の詳細な説明】**

【0001】

【発明の属する技術分野】 この発明は、ユーザ認証時に入力されたユーザ認証情報と、予め設定登録されている

ユーザ認証情報とを照合することによってユーザ認証を行う認証システム、そのプログラム、認証方法に関する。

#### 【0002】

【従来の技術】従来、本人確認を行う認証システムとしては、例えば、図13(a)に示すように、センサシステム(指紋センサ)によって検知された指紋パターンデータがインターネットや構内通信網を介してサーバ側のハードディスク内に個人識別情報(ユーザ認証情報)として登録管理されている状態において、ユーザ認証時には、図13(b)に示すように、センサシステムによって検知された指紋パターンデータと、サーバ側のハードディスク内に設定登録されている指紋パターンデータとを照合し、その照合結果に応じて例えば、コンピュータ装置へのアクセス可否を決定するようにしている。また、独身マンション入室管理システムや建物入館管理システム等においては、本人確認を行う認証システムが備えられており、指紋センサ装置から入力された指紋パターンデータが予めユーザ認証情報として設定登録されている状態において、ユーザ認証時に、指紋センサ装置から指紋パターンデータが入力されると、予め設定登録されているユーザ認証情報(登録情報)と今回入力された指紋パターンデータとを照合することによってユーザ認証を行い、その認証結果に基づいて入室管理や入館管理を行うようにしている。この場合、いずれの認証システムにおいても、登録情報(指紋パターンデータ)は、その対象者である各ユーザ毎にシステム側に一元管理されている。

#### 【0003】

【発明が解決しようとする課題】しかしながら、この種の認証システムにおいては、第三者が例えば、擬似指を使って指紋パターンデータを入力したものとすると、偶発的にヒットするケースもあり、また、登録情報を何らかの方法で盗用されるケースもある等、その安全性が要望されていた。このことは、指紋認識の場合に限らず、音声認識、顔写真認識、眼球認識、パスワード認識等の場合においても同様であった。

【0004】この発明の課題は、設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理することで、設定登録用のユーザ認証情報を効果的に保護することができると共に、設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理したとしても、確実なセキュリティ管理を実現できるようにすることである。

【0005】この発明の手段は、次の通りである。請求項第1記載の発明は、ユーザ認証時に入力されたユーザ認証情報と、予め設定登録されているユーザ認証情報とを照合することによってユーザ認証を行う管理センタ装置と、ユーザ所有のユーザ端末とが通信ネットワークを介して接続されてなる認証システムであって、ユーザ認証情報を分割する分割手段と、この分割手段によって分

割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素を前記ユーザ端末内に設定する登録情報として割り当てる分割情報割当手段と、ユーザ認証を行う場合に、そのユーザ端末内に設定されている登録情報を取得すると共に、前記システム側に設定されている登録情報とを取得する登録情報取得手段と、この登録情報取得手段によって取得したユーザ端末内の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元する復元手段と、この復元手段によって復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行うユーザ認証手段とを具備するものである。したがって、請求項1記載の発明においては、設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理することで、設定登録用のユーザ認証情報を効果的に保護することができると共に、設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理したとしても、確実なセキュリティ管理を実現することができる。

【0006】なお、この発明は次のようなものであってもよい。複数のユーザに対応してそれらのユーザ認証情報をそれぞれ設定登録する場合において、前記分割手段によって分割されたユーザ認証情報の構成要素をユーザ側の登録情報として当該ユーザ端末内に設定させる際には、このユーザ側の登録情報がシステム側のどの登録情報に対応するかを示す為の識別情報を含めて当該ユーザ側の登録情報を設定させ、ユーザ認証を行う場合に、前記登録情報取得手段は、そのユーザ所有のユーザ端末内に設定されているユーザ側の登録情報と共に前記識別情報を取得し、この識別情報に基づいて対応するシステム側の登録情報を取得する(請求項2記載の発明)。

【0007】ユーザ認証を行った後において、前記分割手段は、前回の分割方法とは異なる方法でユーザ認証情報を再分割し、前記分割情報割当手段は、この分割手段によって再分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素をユーザ端末内に設定するユーザ側の登録情報として割り当てることにより、前回のユーザ側の登録情報とシステム側の登録情報の内容を変更する(請求項3記載の発明)。この場合、ユーザ認証が行われる毎に、前記分割手段は、ユーザ認証情報の分割位置をランダムに決定すると共に、この決定された分割位置にしたがってユーザ認証情報を再分割する(請求項4記載の発明)。

【0008】ユーザの特徴情報をユーザ認証情報として検知する検知装置を設け、この検知装置とユーザ所持の携帯通信装置との間で近距離無線通信を行うと共に、前記携帯通信装置は、前記検知装置によって検知されたユーザ認証情報を受信して前記管理センタ装置へ送信し、前記管理センタ装置は、前記携帯通信装置から送信され

て来たユーザ認証情報を分割すると共に、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素を前記ユーザ端末内に設定するユーザ側の登録情報として割り当てる（請求項5記載の発明）。

【0009】前記分割手段は、ユーザ認証情報を複数の分割位置で分割し、前記分割情報割当手段は、前記複数の分割位置によって細かく分割されたユーザ認証情報の各構成要素のうち、システム側に割り当てるべき構成要素と、ユーザ端末内に割り当てるべき構成要素を選択決定する（請求項6記載の発明）。

【0010】他の発明は、コンピュータに対して、上述した請求項1記載の発明に示した主要機能を実現させるためのプログラムを提供し（請求項7記載の発明）、また、上述した請求項1記載の発明に示した主要手順にしたがった処理を行う認証方法を提供するものである（請求項8記載の発明）。

【0011】

【発明の実施の形態】以下、図1～図11を参照してこの発明の一実施形態を説明する。図1は、この実施形態における認証システムの全体構成を示したブロック図である。この実施形態における認証システムは、マンション入室管理システムに採用したもので、一般参加の募集に応じて参加申込のあった各利用者（マンションの管理者）側との間で利用契約を行って会員登録を行い、その会員マンションの各入居者に対するユーザ認証サービスを代行するサービス事業を全国規模で展開するようにした広域通信システムである。このようなユーザ認証サービスを代行する認証システムは、ユーザ認証サービスを行う認証管理センタ1と、各会員マンションの各入居者（ユーザ）所持のユーザ端末（携帯電話端末）2とがネットワーク網（インターネット）3、移動体通信網4を介して接続されているシステム環境となっている。

【0012】認証管理センタ1は、このセンタの中核をなす管理サーバ11と、ユーザデータベースDBを管理制御するデータベースサーバ12と、電子メールを管理制御するメールサーバ13と、Webサーバ14等の各種サーバを有し、これらのサーバによってこの認証管理センタ1の全体動作を制御するようにしている。なお、この実施形態においては、例えば、TCP/IP通信プロトコルを利用したHTTPプロトコル等によって、認証管理センタ1とユーザ端末2との間でデジタル化（パケット化）されたデータの送受信を行うようにしており、また、コード化された制御情報を含むデータによって互に必要な処理内容を認識しながら連携し合ってデータ処理を行うようにしている。なお、ユーザ端末2は、Webブラウザ機能を備えている。

【0013】会員マンション側には、指紋センサ装置5が配置されている。この指紋センサ装置5は、会員登録を行った会員マンションに対し有料にて設置されたもの

で、会員マンションの各入居者を管理するマンション入室管理システム（図2参照）に接続されている。この指紋センサ装置5は、その会員マンションの各入居者所持のユーザ端末（携帯電話端末）2との間において近距離通信によってデータの送受信を行うようにしている。すなわち、近距離通信手段としては、微弱通信規格のBluetooth無線通信や赤外線通信規格のIrDA無線通信によって指紋センサ装置5と各入居者所持のユーザ端末2との間でデータの送受信を行うようにしている。この場合、認証管理センタ1と指紋センサ装置5とは、ユーザ端末2および広域通信網（インターネット3、移動体通信網4）を介してデータの送受信を行うようにしている。

【0014】図2は、指紋センサ装置5の全体構成を示したブロック図である。指紋センサ装置5は、指の指紋を検知する光センサ（エリアセンサ）5-1を有し、このエリアセンサ5-1からの検知信号は、フィルタ5-2、サンプリングホールド部5-3を介してA/D変換部5-4に与えられ、A/D変換部5-4によって変換されたデジタルデータは、特徴抽出部5-5によってユーザ固有の指紋パターンデータに変換され、バッファ5-6を介して近距離無線送信部5-7からユーザ端末2へ送信される。

【0015】また、指紋センサ装置5には、ユーザ端末2から近距離無線通信によって送信されて来たデータを受信する近距離無線受信部5-8が設けられており、この近距離無線受信部5-8によって受信したデータは、バッファ5-9を介して認証結果判定部5-10に与えられる。認証結果判定部5-10は、認証管理センタ1からユーザ端末2を介して送信されて来た認証結果を判別し、認証NG（否定）、認証OK（肯定）に応じた判定信号を生成出力するもので、この判定信号はマンション入室管理システム6に送信される。なお、マンション入室管理システム6は、会員マンションである各入居者の入室状況を管理する通常の管理システムである。

【0016】図3（A）は、ユーザデータベースDBの内容を示した図である。このユーザデータベースDBは、会員マンションの各入居者に対応して、「氏名」、「連絡先」、「ユーザID」、「分割登録パターン」、「復元キー」等の各項目を有するユーザレコードを記憶管理する構成となっている。「氏名」は入居者の氏名、「連絡先」は入居者の電話番号や電子メールアドレスであり、「ユーザID」は、ユーザ登録時に認証管理センタ1側から割り当てられたユーザ固有の識別情報である。

【0017】また、「分割登録パターン」は、ユーザ認証用として予め設定登録されるユーザ認証情報（指紋パターンデータ）を分割した各構成要素のうち、その一方の構成要素パターンである。すなわち、この実施形態においては、ユーザ認証用として設定登録されるユーザ認

証情報（指紋パターンデータ）を2分割して分散管理するようにしており、その一方の構成要素パターンをシステム側の登録情報として割り当てると共に、他方の構成要素パターンをユーザ側の登録情報として割り当てて設定登録するようにしている。この場合、ユーザデータベースDB内の「分割登録パターン」は、上述したシステム側の登録情報である。

【0018】「復元キー」は、ユーザ側の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を合成復元する際に使用する為の復元用の情報であり、この実施形態においては、設定登録用のユーザ認証情報を分割した分割位置を示す情報である。この実施形態においては、ユーザ認証情報（指紋パターンデータ）を2分割する場合、その分割位置を「復元キー」として登録しておき、復元時にはこの「復元キー」によって示される分割位置にしたがってユーザ側の登録情報とシステム側の登録情報とを合成復元するようにしている。

【0019】図3（B）は、ユーザ認証情報（指紋パターンデータ）を2分割することによって得られた他方の構成要素パターンがユーザ側の登録情報として記憶管理されている状態を示した図である。ここで、「ユーザ登録済みフラグ」は、ユーザ側の登録情報がそのユーザ端末2内に登録済みであることを示すフラグである。また、ユーザ側の登録情報は、「分割登録パターン」に「ユーザID」を付加してユーザ端末2内のメモリに記憶管理されている。

【0020】図4は、ユーザ端末2から認証管理センタ1へ送信される伝送フォーマットを示したもので、

（A）は、ユーザ登録時の伝送フォーマット、（B）はユーザ認証時の伝送フォーマットを示している。ユーザ登録時の伝送フォーマットは、「ヘッダー」、「登録」、「レングスL」、「指紋パターンデータ」、「ユーザID」の各データからなり、「指紋パターンデータ」は、設定登録用のユーザ認証情報であり、「レングスL」は「指紋パターンデータ」のデータ長を示している。ユーザ認証時の伝送フォーマットは、「ヘッダー」、「認証」、「今回入力指紋パターンデータ」、「ユーザ既登録パターン」、「ユーザID」の各データからなり、「ユーザ既登録パターン」は、上述したユーザ側の登録情報である「分割登録パターン」であり、「今回入力指紋パターンデータ」は、ユーザ認証時に検知されたデータである。

【0021】図5は、認証管理センタ1の中核を成す管理サーバ11の全体構成を示したブロック図である。CPU111は、記憶装置112内のオペレーティングシステムや各種アプリケーションソフトにしたがってこの管理サーバ11の全体動作を制御する中央演算処理装置である。記憶装置112は、オペレーティングシステムや各種アプリケーションソフト等が格納され、磁氣的、光学的、半導体メモリ等によって構成されている記録媒

体113やその駆動系を有している。この記録媒体113はハードディスク等の固定的な媒体若しくは着脱自在に装着可能なCD-ROM、フロッピーディスク、RAMカード、磁気カード等の可搬型の媒体である。また、この記録媒体113内のプログラムやデータは、必要に応じてCPU111の制御によりRAM（例えば、スタティックRAM）114にロードされたり、RAM114内のデータが記録媒体113にセーブされる。更に、記録媒体は外部機器側に設けられているものであってもよく、CPU111は伝送制御部115を介してこの記録媒体内のプログラム／データを直接アクセスして使用することもできる。

【0022】また、CPU111は記録媒体113内に格納されるその一部あるいは全部を他の機器側から伝送制御部115を介して取り込み、記録媒体113に新規登録あるいは追加登録することもできる。更に、プログラム／データはサーバ等の外部機器側で記憶管理されているものであってもよく、CPU111は伝送制御部115を介して外部機器側のプログラム／データを直接アクセスして使用することもできる。一方、CPU111にはその入出力周辺デバイスである伝送制御部115、入力部116、表示部117がバスラインを介して接続されており、入出力プログラムにしたがってCPU111はそれらの動作を制御する。

【0023】図6は、ユーザ端末2の全体構成を示したブロック図である。なお、ユーザ端末2の構成要素も上述した管理サーバ11の構成要素に対応して、CPU201、記憶装置202、RAM203、入力部204、表示部205の他、近距離無線通信部206、広域無線通信部207を有する構成となっている。近距離無線通信部206は、指紋センサ装置5との間でBluetooth無線通信やIrDA無線通信によってデータの送受信を行うものであり、広域無線通信部207は、認証管理センタ1との間でインターネット3、移動体通信網4を介してデータの送受信を行うものである。

【0024】次に、この実施形態における認証システムの動作アルゴリズムを図7～図10に示すフローチャートを参照して説明する。ここで、これらのフローチャートに記述されている各機能、つまり、図7に記述したユーザ登録処理、図8および図9に記述したユーザ認証処理、図10に記述したユーザ端末側の処理は、読み取り可能なプログラムコードの形態で格納されており、認証管理センタ1やユーザ端末2は、このプログラムコードにしたがった動作を逐次実行する。また、伝送媒体を介して伝送されてきた上述のプログラムコードにしたがった動作を逐次実行することもできる。すなわち、記録媒体の他、伝送媒体を介して外部供給されたプログラム／データを利用してこの実施形態特有の動作を実行することもできる。

【0025】図7～図9は、認証管理センタ1側におい

て実行される動作を示したフローチャートであり、図 10 は、ユーザ端末 2 側の主要動作（この実施形態固有の動作）を示したフローチャートである。まず、認証管理センタ 1 側でのユーザ登録処理と、この登録処理にตอบสนองして実行されるユーザ端末 2 側での動作を説明する。いま、登録会員であるマンションの入居者であるユーザは、自己のユーザ端末 2 から認証管理センタ 1 に対してユーザ登録要求を行うが、この場合、「ユーザ登録済みフラグ」を参照し、「ユーザ登録済みフラグ」がオンされているかをチェックし（図 10 のステップ D 1）、当該フラグがオフされていることを条件にユーザ登録指示を受け付け（ステップ D 2）、認証管理センタ 1 に対してユーザ登録要求を行う（ステップ D 3）。

【0026】認証管理センタ 1 は、ユーザからの登録アクセス待ち状態において（図 7 のステップ A 1）、いずれかのユーザ端末 2 から登録要求を受信すると、ユーザ登録入力ページを要求元のユーザ端末 2 へ送信する（ステップ A 2）。ユーザ端末 2 は、このユーザ登録入力ページを受信すると（図 10 のステップ D 4）、その入力ページ画面を表示出力させる（ステップ D 5）。このユーザ登録入力ページ画面は、「登録会員マンション名」の他に、その入居者の「氏名」、「連絡先」等の各項目に対応してその入力領域を有するもので、このページ画面内に必要事項を入力した後、当該ページ画面内の送信ボタンを操作すると、入力されたユーザ情報は、認証管理センタ 1 へ送信される（ステップ D 6）。

【0027】認証管理センタ 1 は、ユーザ情報を受信すると（図 7 のステップ A 3）、そのユーザに割り当てべきユーザ ID を発行して要求元のユーザ端末 2 へ送信する（図 7 のステップ A 4）。この場合、ユーザ端末 2 は、認証管理センタ 1 から送信されて来たユーザ ID を受信して登録する（図 10 のステップ D 7）。そして、認証管理センタ 1 は、受信したユーザ情報をユーザデータベース DB に追加登録した後（図 7 のステップ A 5）、要求元のユーザ端末 2 へ指紋パターンデータの入力を促す為のメッセージを含む指紋入力通知を行う（ステップ A 6）。

【0028】ユーザ端末 2 は、指紋入力通知を受信すると、そのメッセージ内容を表示出力してユーザに報知する（図 10 のステップ D 8）。ここで、ユーザは、指紋センサ装置 5 のエリアセンサ 5-1 上に指を載せると、フィルタ 5-2、サンプリングホールド部 5-3、A/D 変換部 5-4、特徴抽出部 5-5、バッファ 5-6、近距離無線送信部 5-7 を介してユーザ端末 2 へ指紋パターンデータが送信される。ユーザ端末 2 は、指紋センサ装置 5 によって検知された指紋パターンデータを受信すると（図 10 のステップ D 9）、図 4（A）に示したような登録伝送フォーマットに、「指紋パターンデータ」、「データ長 L」、「ユーザ ID」等を配置した伝送データを作成して認証管理センタ 1 へ送信する（ステ

ップ D 10）。その後、「ユーザ登録済みフラグ」をオンさせる（ステップ D 11）。

【0029】認証管理センタ 1 は、ユーザ端末 2 から送信されて来た登録伝送データを受信すると（図 7 のステップ A 7）、「指紋パターンデータ」、「データ長 L」を抽出し、この「データ長 L」にしたがって「指紋パターンデータ」の midpoint を求め、この midpoint を境に「指紋パターンデータ」を 2 分割する（ステップ A 8）。図 11

（A）は、この場合の分割状態を示した図で、その前半部の分割パターンがシステム側の登録情報となり、後半部の分割パターンがユーザ側の登録情報となる。

【0030】そして、前半部の分割パターン（システム側の登録情報）を「ユーザ ID」と共にユーザデータベース DB に登録する他（ステップ A 9）、「復元キー」を生成してユーザデータベース DB の該当項目に登録する（ステップ A 10）。この場合の「復元キー」は、midpoint 位置情報となる。また、後半部の分割パターンをユーザ側の登録情報として、その「ユーザ ID」と共に、要求元のユーザ端末 2 へ送信する（ステップ A 11）。

【0031】ユーザ端末 2 は、「ユーザ登録済みフラグ」がオンされている状態において（図 10 のステップ D 1）、認証管理センタ 1 からその「ユーザ ID」と共に送信されて来た分割パターン（ユーザ側の登録情報）を受信すると（ステップ D 12）、受信した「ユーザ ID」と予め登録されている自己の「ユーザ ID」とが一致するかを判別し（ステップ D 13）、不一致の場合には、受信データを無視するが、一致する場合には、受信した分割パターン（後半部）を登録する処理を行う（ステップ D 14）。

【0032】図 8 および図 9 は、認証管理センタ 1 側で実行されるユーザ認証処理を示したフローチャートである。以下、認証管理センタ 1 側でのユーザ認証処理と、この認証処理にตอบสนองして実行されるユーザ端末 2 側での動作を図 10 に示すフローチャートを参照して説明する。まず、ユーザ認証時において、ユーザは指紋センサ装置 5 に指を載せると、この指紋センサ装置 5 によって検知された指紋パターンデータは、ユーザ端末 2 へ送信される。ユーザ端末 2 は、指紋センサ装置 5 からの指紋パターンデータを受信すると（図 10 のステップ D 15）、ユーザ側の登録情報である「ユーザ登録分割パターン」と「ユーザ ID」とを取得し（ステップ D 16）、図 4（B）に示したような認証用の伝送フォーマットに、「今回入力した指紋パターンデータ」、「ユーザ登録分割パターン」、「ユーザ ID」等を配置した伝送データを作成して認証管理センタ 1 へ送信する（ステップ D 17）。

【0033】認証管理センタ 1 は、この認証アクセス要求を受信すると（図 8 のステップ B 1）、この受信データの中から「今回入力した指紋パターンデータ」、「ユーザ登録分割パターン」、「ユーザ ID」を抽出し（ステ



ップB2)、この「ユーザID」に基づいてユーザデータベースDBを検索し(ステップB3)、それに該当するシステム側の「登録分割パターン」が有るかを判別し(ステップB4)、無ければ、認証NG(否定)を要求元のユーザ端末2へ送信するが(ステップB11)、有れば、該当するシステム側の「登録分割パターン」と「復元キー」とをユーザデータベースDBから取得する(ステップB5)。そして、この「復元キー」に基づいてパターン展開用の座標系上の合成位置を求め、この位置を基準として、「システム側登録分割パターン」と「ユーザ側登録分割パターン」とを配置して元の「指紋パターンデータ」を合成復元する(ステップB6)。

【0034】そして、認証管理センタ1は、復元した「指紋パターンデータ」と「今回入力の指紋パターンデータ」とを比較し(ステップB7)、両者の一致を判別する(ステップB8)。ここで、不一致の場合には、認証NG(否定)を要求元のユーザ端末2へ送信するが(ステップB11)、一致する場合には、認証OK(肯定)を要求元のユーザ端末2へ送信する(ステップB9)。この場合、ユーザ端末2では、認証管理センタ1からの認証結果を受信すると(図10のステップD18)、その受信結果を表示出力すると共に(ステップD19)、指紋センサ装置5へその認証結果を送信する(ステップD20)。

【0035】指紋センサ装置5において、その近距離無線受信部5-8によって受信したデータがバッファ5-9を介して認証結果判定部5-10に与えられると、認証結果判定部5-10は、認証管理センタ1からユーザ端末2を介して送信されて来た認証結果を判別し、認証NG(否定)、認証OK(肯定)に応じた判定信号を生成出力してマンション入室管理システム6に送信される。

【0036】その後、認証管理センタ1は、認証OK(肯定)の場合には(図8のステップB8)、指紋パターン再登録処理に移る(ステップB10)。図9は、この指紋パターン再登録処理を示したフローチャートである。認証管理センタ1は、乱数発生器(図示せず)からランダム数値を取得し(ステップC1)、このランダム数値に基づいて分割位置を決定する(ステップC2)。例えば、数値“1”～“20”の中から発生されたランダム数値に対応付けられている分割位置を今回の分割位置として決定する。そして、上述のようにして復元された「指紋パターンデータ」を決定位置で再分割する(ステップC3)。

【0037】図11(B)は、ランダム分割された状態を例示した図で、その前部の分割パターンがシステム側の登録情報となり、後部の分割パターンがユーザ側の登録情報となることは、上述の場合と同様であるが、

(A)の場合に比べて、ランダム分割によってその分割位置が異なっている。この場合、システム側の方がユー

ザ側よりもそのデータ長は大きくなっている。なお、

(C)は、次の指紋パターン再登録処理によって分割された状態を例示した図で、更に、その分割位置は異なり、ユーザ側の方がシステム側よりもそのデータ長は大きくなっている。

【0038】そして、認証管理センタ1は、ランダム分割による「復元キー」を生成してユーザデータベースDBの該当項目に登録することによってその内容を変更すると共に(ステップC4)、ランダム分割によって得られた前部の分割パターンをシステム側の登録情報として、ユーザデータベースDBの該当項目に登録することにより前回の内容を変更する(ステップC5)。そして、後部の分割パターンをユーザ側の登録情報として、要求元のユーザ端末2へ送信する(ステップC6)。すると、ユーザ端末2側では、認証管理センタ1から送信されて来たユーザ登録用の分割パターンを受信すると(図10のステップD12)、その「ユーザID」が一致することを条件に(ステップD13)、当該分割パターンを登録することにより、前回の内容を変更する(ステップD14)。

【0039】以上のように、この実施形態において認証管理センタ1は、ユーザ登録時に、指紋センサ装置5からユーザ端末2を介して通信されて来たユーザ認証情報(指紋パターンデータ)を分割すると共に、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素をユーザ側の登録情報として割り当てて設定登録させるようにしたから、設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理することができると共に、例えば、ユーザ端末2内に設定されているユーザ側の登録情報が盗用されたとしても、それは登録情報の一部だけである為にセキュリティ上、問題となることはなく、登録情報を効果的に保護することが可能となる。

【0040】この場合、ユーザ認証時ににおいて認証管理センタ1は、当該ユーザ端末2に設定されているユーザ側の登録情報を取得すると共に、認証管理センタ1のユーザデータベースDBに設定されているシステム側の登録情報とを取得し、取得したユーザ側の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元した後、復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行うようにしたから、設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理したとしても、ユーザ認証を確実に行うことが可能となる。

【0041】また、複数のユーザに対応してそれらのユーザ認証情報をそれぞれ設定登録する場合において、認証管理センタ1は、分割したユーザ認証情報の構成要素をユーザ側の登録情報としてユーザ端末2に設定登録させる際に、このユーザ側の登録情報がシステム側のどの



登録情報に対応するかを示す為の識別情報（ユーザID）を含めてそのユーザ側の登録情報を設定し、ユーザ認証を行う場合には、そのユーザ端末2に設定されているユーザ側の登録情報と共にユーザIDを取得し、このユーザIDに基づいて対応するシステム側の登録情報を取得して復元処理を行うようにしたから、複数ユーザに対応してそれらの登録情報を分散管理したとしても、ユーザ別ユーザ認証を確実に行うことが可能となる。

【0042】また、ユーザ認証を行った後において、認証管理センタ1は、前回の分割方法とは異なる方法でユーザ認証情報を再分割するようにしたから、分散管理される登録情報をユーザ認証毎に変更することができ、盗用等から登録情報を効果的に保護することができる。この場合、ユーザ認証情報の分割位置をランダムに決定し、その分割位置にしたがって再分割するようにしたから、より確実な保護が可能となる。

【0043】また、ユーザの特徴情報である指紋を検知する指紋センサ装置5と、そのユーザ所持の携帯電話（ユーザ端末2）との間で近距離無線通信を行うようにしたから、つまり、本人だけが所持する携帯電話を介して指紋センサ装置5と認証管理センタ1との間でデータの送受信を行うようにしたから、第三者が介入する余地が無くなり、また、携帯電話を紛失したり、盗難されたとしても、携帯電話に設定されている登録情報は、その一部であるために安全性を確保することができる。

【0044】なお、上述した実施形態においては、ユーザ認証情報を2分割する場合を示したが、図12に示すように、3分割するようにしてもよく、分割数は任意である。この場合、ユーザ認証情報を複数の分割位置で分割し、この複数位置によって細かく分割されたユーザ認証情報の各構成要素のうち、システム側に割り当てるべき構成要素と、ユーザ側に割り当てるべき構成要素を任意に選択して決定するようにしてもよい。例えば、システム側に割り当てるべき構成要素とユーザ側に割り当てるべき構成要素とを交互に決定したり、任意に選択して決定して分散管理させるようにしてもよい。

【0045】また、上述した実施形態における認証システムは、マンション入室管理システム6に連動するようにしたが、これに限らず、パーソナルコンピュータをオープンする際に、ユーザ認証を行ってアクセス可否を制御する者であってもよい。また、ユーザ認証情報としては、指紋パターンデータに限らず、音声認識、顔写真認識、眼球認識、パスワード認識等をユーザ認証情報としてもよい。更に、ユーザ個人の認証に限らず、グループ認証等であってもよい。

【0046】一方、コンピュータ（認証管理センタ1）に対して、上述した各手段を実行させるためのプログラムコードをそれぞれ記録した記録媒体（例えば、CD-ROM、フロッピディスク、RAMカード等）を提供するようにしてもよい。すなわち、コンピュータが読み取

り可能なプログラムコードを有する記録媒体であって、ユーザ認証情報を分割する機能と、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報とすると共に、他方の構成要素をユーザ側の登録情報として設定する機能と、ユーザ認証を行う場合に、当該ユーザ端末に設定されているユーザ側の登録情報を取得すると共に、前記システム側に設定されているシステム側の登録情報とを取得する機能と、取得したユーザ側の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元する機能と、復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行う機能とを実現させるためのプログラムを記録したコンピュータが読み取り可能な記録媒体を提供するようにしてもよい。

【0047】

【発明の効果】この発明によれば、ユーザ登録時に、ユーザ端末を介して通信されて来たユーザ認証情報を分割すると共に、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報とすると共に、他方の構成要素をユーザ側の登録情報として設定させるようにしたから、設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理することができる。したがって、例えば、ユーザ端末に設定されているユーザ側の登録情報が盗用されたとしても、それは登録情報の一部だけである為にセキュリティ上、問題となることはなく、登録情報を効果的に保護することが可能となる。この場合、ユーザ認証時においてユーザ端末に設定されているユーザ側の登録情報を取得すると共に、システム側の登録情報とを取得し、取得したユーザ側の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元した後、復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行うようにしたから、設定登録用のユーザ認証情報を複数の分割して分散管理したとしても、ユーザ認証を確実に行うことが可能となる。

【図面の簡単な説明】

【図1】認証システムの全体構成を示したブロック図。

【図2】指紋センサ装置5の全体構成を示したブロック図。

【図3】（A）は、ユーザデータベースDBの内容を示した図、（B）は、ユーザ認証情報（指紋パターンデータ）を2分割することによって得られた他方の構成要素パターンがユーザ側の登録情報として記憶管理されている状態を示した図。

【図4】ユーザ端末2から認証管理センタ1へ送信される伝送フォーマットを示し、（A）は、ユーザ登録時の伝送フォーマット、（B）はユーザ認証時の伝送フォーマットを示した図。

【図5】認証管理センタ1の中核を成す管理サーバ11の全体構成を示したブロック図。

【図6】ユーザ端末2の全体構成を示したブロック図。

【図7】認証管理センタ1側において実行されるユーザ登録処理を示したフローチャート。

【図8】認証管理センタ1側で実行されるユーザ認証処理を示したフローチャート。

【図9】上述のユーザ認証処理において実行される指紋パターン再登録処理を示したフローチャート。

【図10】ユーザ端末2側の主要動作（この実施形態固有の動作）を示したフローチャート。

【図11】(A)は、ユーザ登録時における指紋パターンデータの分割状態を示した図、(B)は、指紋パターン再登録処理によってランダム分割された指紋パターンデータの分割状態を例示した図、(C)は、次の指紋パターン再登録処理によってランダム分割された状態を例示した図。

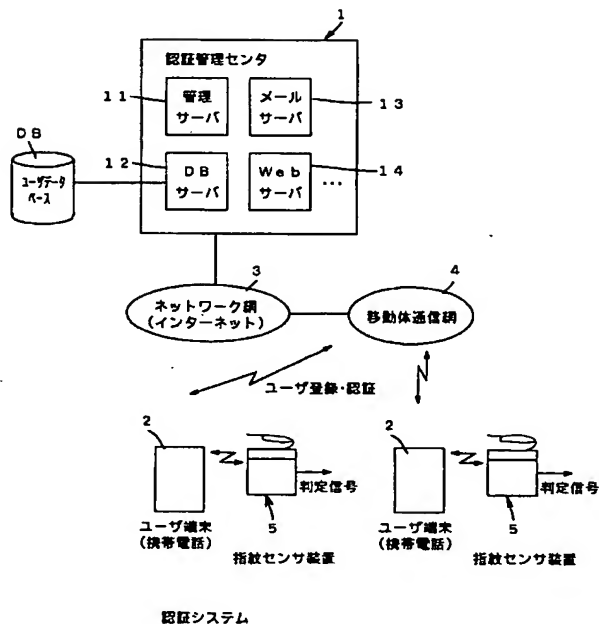
【図12】指紋パターンデータを分割して登録する場合の変形応用例を示した図。

【図1-3】(a)、(b)は、従来例を説明する為の図。

【符号の説明】

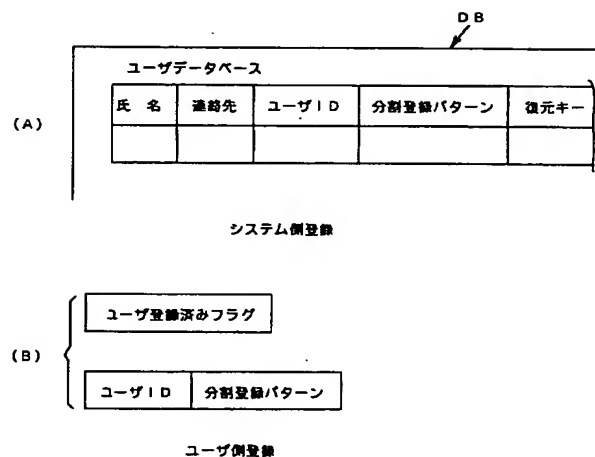
- 1 認証管理センタ
- 2 ユーザ端末
- 3 ネットワーク網
- 4 移動体通信網
- 5 指紋センサ装置
- 6 マンション入室管理システム
- 11 管理サーバ
- 12 データベースサーバ
- 13 メールサーバ
- 14 Webサーバ
- 5-7 近距離無線送信部
- 5-8 近距離無線受信部
- 5-10 認証結果判定部
- DB ユーザデータベース
- 111、201 CPU
- 112、202 記憶装置
- 113 記録媒体
- 115 伝送制御部
- 206 近距離無線通信部
- 207 広域無線通信部

【図1】

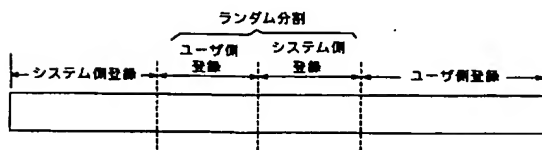


認証システム

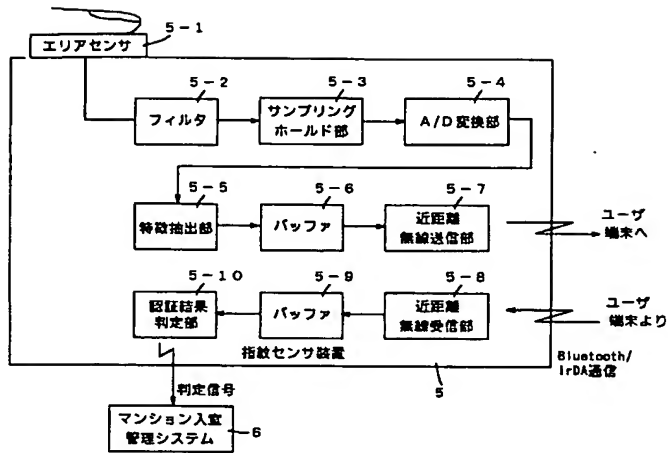
【図3】



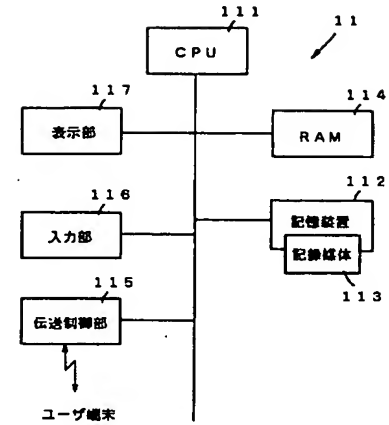
【図12】



【図2】

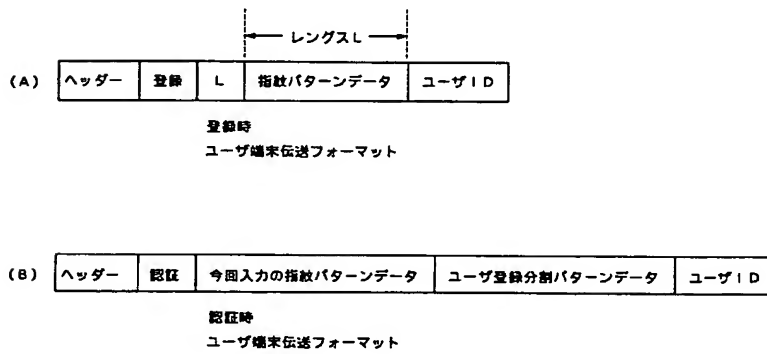


【図5】

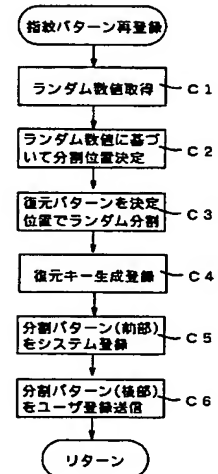


管理サーバ

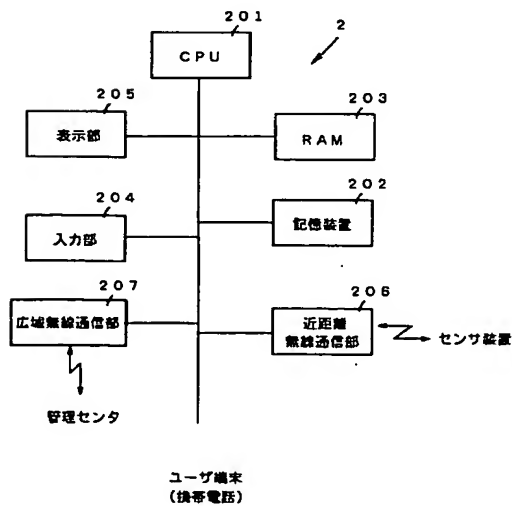
【図4】



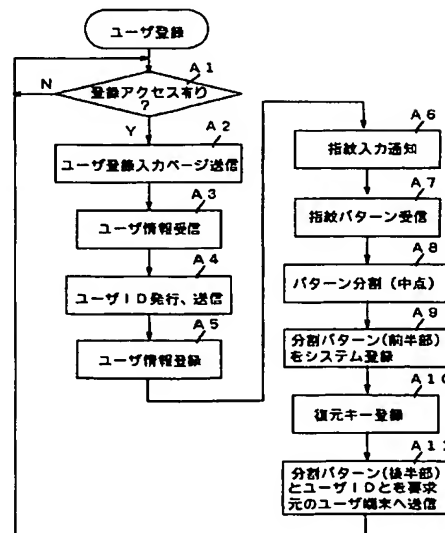
【図9】



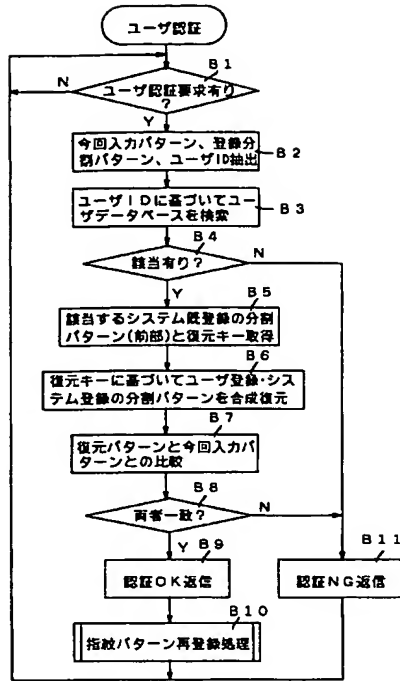
【図6】



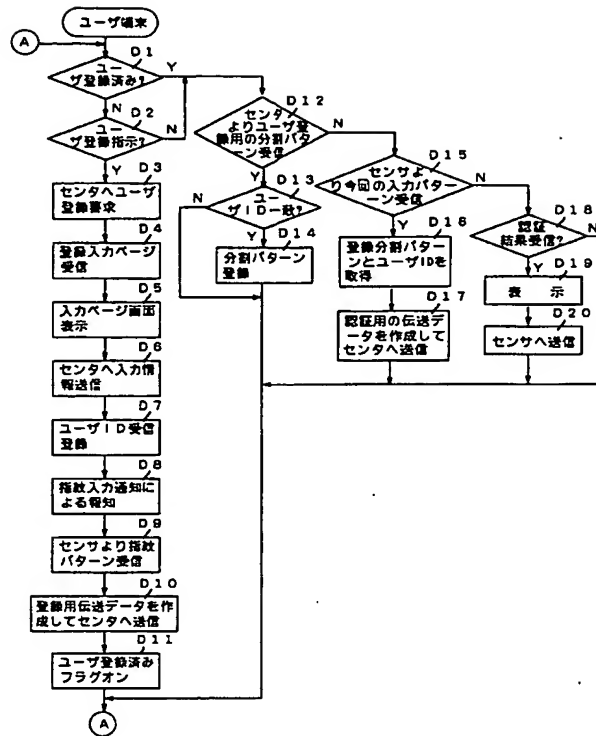
【図7】



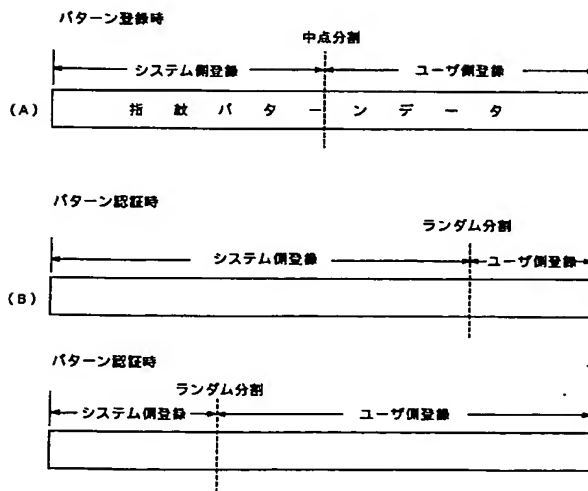
【図 8】



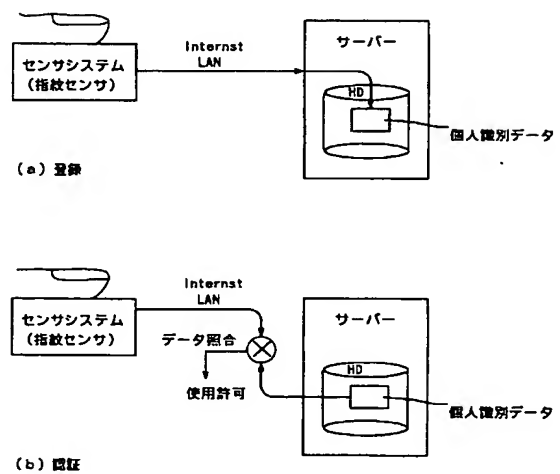
【図 10】



【図 11】



【図 13】



フロントページの続き

(51)Int.C1.7

識別記号

F I  
H 0 4 L 9/00

テーマコード (参考)

6 0 1 D